DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

REMARKS

The following Request for Reconsideration is submitted in response to the

Final Office Action issued on October 28, 2004 (Paper No. unknown) in connection with the

above-identified patent application, and is being filed within the three-month shortened

statutory period set for a response by the Office Action.

Claims 106-181 remain pending in the present application, and stand finally

rejected. Applicants respectfully request reconsideration and withdrawal of the final rejection

of such claims.

Preliminarily, Applicants respectfully note that the Examiner includes within

the Final Office Action at pages 2 and 3 thereof a section entitled "Official Notice Traversal".

However, inasmuch as Applicants are not aware that the Examiner has specifically taken

Official Notice of anything in particular in connection with the present application,

Applicants are puzzled as to the purpose of such section. Thus, Applicants respectfully

request clarification.

Also, Applicants respectfully note that the Examiner includes within the Final

Office Action at page 3 thereof a section entitled "Examiner's Note". According to such

section, the Examiner requests that in addition to the cited portions of the applied reference,

Applicants should fully consider the entirety of the reference as "potentially teaching all or

part of the claimed invention". Applicants respectfully decline to do so inasmuch as it is the

Examiner's responsibility and not Applicants' to make a prime facie showing in connection

with a rejection of the claims.

Applicants are entitled to a full and complete examination from the Examiner,

and are not required to assist the Examiner in ascertaining any 'potential teachings' that by no

DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

means necessarily exist and that at any rate the Examiner has not considered worthy enough to be specifically pointed out. Further Applicants respectfully submit that such statement is in fact an acknowledgment that the Examiner has not set forth a prime facie showing in connection with the rejection of the claims.

That said, the Examiner has finally rejected claims 106-181 under 35 USC § 103(a) as being obvious over Downs et al. (U.S. Patent No. 6,574,609). Applicants respectfully traverse the § 103(a) rejection of claims 106-181.

Again, independent claim 106 recites a method in combination with a digital rights management (DRM) system operating on a computing device, where the DRM system employs a black box for performing decryption and encryption functions. The method is for obtaining the black box by the DRM system from a black box server. In the method, the DRM system requests the black box from the black box server and the black box server generates the black box, where such generated black box has a unique public / private key pair. The black box server then delivers the generated black box to the DRM system, and the DRM system installs the delivered black box therein.

Independent claim 122 recites subject matter similar to that in independent claim 106, but from the point of view of the DRM system. Independent claim 138 recites subject matter similar to that in independent claim 106, but from the point of view of the black box server. Independent claim 152 recites subject matter similar to that in independent claim 122, but in the form of a computer-readable medium having computer-executable instructions thereon for performing the method of claim 122. Independent claim 168 recites subject matter similar to that in independent claim 138, but likewise in the form of a

computer-readable medium having computer-executable instructions thereon for performing

the method of claim 138.

Applicants again respectfully submit that in setting forth the present

rejection under section 103, the Examiner is impermissibly equating the recited black

box as merely a set of encryption / decryption keys. Instead, the present application and

the recited claims are quite clear that the recited black box includes such keys <u>and</u> the

functionality necessary to employ same in a particular manner within the DRM system

on the computing device. Thus, Applicants respectfully submit that interpreting the

recited black box to be merely a set of keys is improper inasmuch as the claims and

specification of the present application clearly require otherwise.

Again, the black box as recited in the claims is a device that performs

encryption and decryption for the DRM system as part of such DRM system, and that

employs the unique public / private key pair and other cryptographic keys to perform such

encryption and decryption. As is set forth in the specification of the present application, the

black box is constructed and proffered in a particular manner so as to be trusted by the DRM

system to perform the decryption and encryption functions for such DRM system, and also

includes a version number and a unique signature, all as provided by an approved certifying

authority.

The public key of the black box is made available to a license server for

purposes of encrypting portions of the issued license, thereby binding such license to such

black box. The private key is available to the black box only, and not to the user or anyone

else, for purposes of decrypting information encrypted with the corresponding public key.

The black box as received from the black box server is written in unique executable code that

will run only on the user's computing device, and is intended to be replaced on a regular basis

by newer black boxes. (Application, at page 4.)

The black box 30 works in conjunction with the license evaluator 36 to

decrypt and encrypt certain information as part of the license evaluation function. In

addition, once the license evaluator 36 determines that a user does in fact have the right to

render the requested digital content 12 in the manner sought, the black box 30 is provided

with a decryption key (KD) for such digital content 12, and performs the function of

decrypting such digital content 12 based on such decryption key (KD). The license server 24

must trust that the black box 30 will perform the decryption function only in accordance with

the license rules in the license 16, and also trust that such black box 30 will not operate

should it become adulterated or otherwise modified by a user for the nefarious purpose of

bypassing actual evaluation of a license 16. Accordingly, the black box 30 is also run in a

protected or shrouded environment such that the user is denied access to such black box 30.

(Application, pages 23-24.)

To again summarize, then, Applicants respectfully submit that the Examiner

should not and cannot merely characterize the recited black box of the claims as being with

regard to encryption / decryption keys only. Instead, the recited black box is not merely a set

of keys, but is a device that has a set of keys associated therewith and that performs

cryptographic functions for the DRM system based at least in part on the associated set of

keys. Applicants again respectfully submit that the failure of the Examiner to consider the

claims of the present application in terms of the recited black box and not in terms of keys is

prima facie improper as ignoring the plain language of the claims and also the specification

supporting the claims, and for this reason alone the final rejection should be withdrawn.

DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

Turning now to the Downs reference, Applicants again point out that such Downs reference discloses a system of managing protected content. The content is in the form of a secure container (SC) which includes the content encrypted by a symmetric key that is in turn encrypted by the recipient's public key, various digests, a digital certificate of the sender, and a signature. As seen in Fig. 1D, a recipient of the secure container employs a device 109 that includes a decryption / re-encryption function 194 that is protected with tamper resistant code technology and that serves the purpose of decrypting and re-encrypting the content in a more amenable format and with a more amenable symmetric key. (Column 79, line 38 – column 80, line 14).

Significantly, although the Downs decryption / re-encryption function 194 acts in many respects as the black box of the present application, such Downs reference does not at all disclose or even recognize that such a decryption / re-encryption function 194 can become compromised over time and thus should be updated on a regular basis with a new a decryption / re-encryption function 194 from an appropriate server. **In fact, Applicants respectfully submit that the Downs reference does not even disclose or suggest any method or mechanism by which the function 194 could be so updated. Likewise, and again, Applicants respectfully submit that the Downs reference does not disclose or even suggest any such server for updating the decryption / re-encryption function 194.**

Thus, and again, Applicants respectfully submit that the Downs reference does not disclose or suggest that the Downs end-user device 109 should or could request an updated system decryption / re-encryption function 194 from an appropriate server, as is required by claims 106 et seq., or that such an appropriate server should or could generate same with a unique public / private key pair and deliver the generated function 194 to the

DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

device 109 such that the device 109 installs the delivered function 194 therein, as is also

required by claims 106 et seq. Put simply, without appreciating that the function 194 should

be updatable, the Downs reference simply fails to disclose or even suggest any mechanism by

which such updating can take place.

Applicants note that the Examiner may attempt to infer the delivery and

installation of the Downs function 194 as part of the delivery and installation of the Downs

system on a user's computing device. However, and significantly, such an interpretation fails

inasmuch as such delivery and installation would not be in response to a request for the

function 194 from the Downs system, as is required by the claims. Put simply, the Downs

system cannot make such a request if such Downs system has not as yet been delivered and

installed, Moreover, the Downs reference does not disclose or even suggest any scenario

whereby the Downs system is partially delivered and installed without the function 194, and

then requests same.

In fact, the entirety of the disclosure with regard to the function 194 is at

column 79, line 26 through column 80, line 14 where it is stated that:

> After inscribing any required watermark to this content buffer, the buffer is
> passed to the scrambling function for Re-Encryption 194. A processor efficient secure
> encryption algorithm such as IBM's SEAL encryption technology is used to re-
> encrypt the Content 113 using a random Symmetric Key. Once the download and
> Decryption and Re-Encryption 194 process is complete, the encryption Key 623 used
> by the Content Provider(s) 101 to originally encrypt the Content 113 is now destroyed
> and the new SEAL key is itself encrypted using the Secret User Key created and
> hidden at installation time. This new encrypted Seal Key is now stored in the License
> Database 107.

> The Decryption and Re-Encryption 194 process is another area of the code
> that is protected with Tamper Resistant Code technology so as not to divulge the
> original Content 113 encryption key, the new SEAL key, the Secret User Key, and
> where the Secret User Key segments are stored and how the key is segmented.

DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

The process of Decryption and Re-Encryption 194 serves two purposes. Storing the Content 113 encrypted with an algorithm like SEAL enables faster than real-time decryption and requires much less processor utilization to perform the decryption than does a more industry standard type algorithm like DES. This enables the Player Application 195 to perform a real-time concurrent decryption-decode-playback of the Content 113 without the need to first decrypt the entire file for the Content 113 prior to decode and playback. . . .

The second purpose of this Decryption and Re-Encryption 194 process is to remove the requirement that the original master encryption Key 623, used by the Content Provider(s) 101 to encrypt this Content 113, be stored on every End-User Device(s) 109 which has licensed this Content 113. The encrypted master Key 623, as part of the License SC(s) 660, is only cached on the hard disk of the End-User Device(s) 109 for a very short time and is in the clear only in memory and for a very short time. During this execution phase, the Key 623 is protected via Tamper Resistant Code technology. Not having to retain this Key 623 in any form on the End-User Device(s) 109 once this Decryption and Re-Encryption 194 phase has completed, greatly lessens the possibility of piracy from hackers.

Clearly, no disclosure or suggestion is set forth for how the function 194 is procured, or even that such function 194 should or even could be updated from an appropriate server to include a new key pair, as is required by the claims of the present application. Instead, all that is set forth in connection with function 194 is two purposes without any disclosure of how such function 194 is actually caused to be delivered, installed, and/or instantiated. Thus, Applicants respectfully submit that the disclosure of the function 194 in the Downs reference is not sufficient to teach or even suggest the delivery and installation of the black box of the present invention as recited in the claims of the present application.

Finally, Applicants respectfully note that the Examiner states at page 6 of the Office Action that the present invention as recited in at least claim 106 would be obvious based on the Downs reference because the claimed features would "improve a level of security for a digital rights management system". However, Applicants respectfully submit that such a rationale cannot be employed to support a conclusion of obviousness, if only because such a rationale is actually a result of the present invention, and is not a motivation

DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

that would suggest the present invention to the relevant public in combination with the

Downs reference. Put more simply, Applicants respectfully submit that the Examiner has

impermissibly concluded that since the result of the present invention is desirable, the present

invention must be obvious. For this additional reason, the obviousness rejection of the claims

should be withdrawn.

Accordingly, for all of the aforementioned reasons, Applicants respectfully

submit that the Downs reference cannot be applied to make obvious independent claims 106,

122, 138, 152, and 168, or any claims depending therefrom. Accordingly, Applicants

respectfully request reconsideration and withdrawal of the § 103(a) rejection.
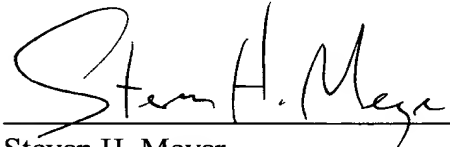
DOCKET NO.: MSFT-0109/127334.9
Application No.: 09/482,840
Office Action Dated: October 28, 2004

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

In view of the foregoing discussion, Applicants respectfully submit that the

present application, including claims 106-181, is in condition for allowance, and such action

is respectfully requested.

Respectfully submitted,

Date: January 17, 2005

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439